UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/955,222	09/19/2001	Richard Brown	1509-220	8293

22879   7590   07/13/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
DINH, KHANH Q

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 07/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/955,222	BROWN ET AL.
	Examiner	Art Unit	
	Khanh Dinh	2151	.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _15 April 2005_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-16_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   This is in response to the Amendment filed on 4/15/2005. Claims 1-16 are

presented for examination.

Claim Objections

2.   Claim 10 is objected to because of the following informalities:

In the claim, "authoriser" should be changed to "authorizer" and "authorising" be

changed to "authorizing".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the

claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the

various claims was commonly owned at the time any inventions covered therein were

made absent any evidence to the contrary. Applicant is advised of the obligation under

37 CFR 1.56 to point out the inventor and invention dates of each claim that was not

commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

4.   Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Spies et al., US pat. No.5,689,565 in view of Scheidt et al., US pat. No.6,754,820.

As to claim 1, Spies discloses a credential transfer method for use on a distributed

electronic network, the method comprising the steps of a sender (participant 22a fig.1)

communicating to a recipient (Participant 22b fig.1) a credential index comprising an

index referring to at least one credential (sending and exchanging users' credential

information), the index including user-provided information about the credential by

selecting at least one of the credentials from the index of at least one credential

provided by the sender (see fig.1, abstract, col.5 line 21 to col.6 line 24), the recipient

(22a fig.1) communicating to the sender (22b fig.1) an indication of the selected at least

one credential and the sender providing to the recipient at least one credential

corresponding to the selected at least one credential (providing secure and credential

information between participants, see also fig.2, col.6 line 36 to col.7 line 28).

Spies does not specifically disclose an index further comprising credential information

differing substantially from the credential such that the credential is not disclosed by the

index. However, Scheidt discloses an index further comprising credential information

differing substantially from the credential (credential that restrict access) such that the

credential is not disclosed by the index (using selecting "Secret" from the security level

category as a credential during encryption would limit readership of the encrypted object

to those who have read access to the "Secret" credential, see fig.3, col.5 line 31 to col.6

line 58 and col.10 lines 10-65). It would have been obvious to one of the ordinary skill

in the art at the time the invention was made to implement Scheidt's secrete credentials
into the computer system of Spies to restrict accesses to data information because it
would have provided sensitivity level or multiple-level access control such that access to
credentials id dependant on the method of member identification and enforced domain
authority dictated policies for multiple-level access control by credential category.

As to claim 2, Spies discloses the recipient responding to the credential index by
determining whether the at least one credential is sufficient and the recipient
communicating the result of the determination to the sender (see fig.2, col.7 line 17 to
col.8 line 28).

As to claim 3, Spies discloses the recipient responding to the credential index by
determining a service level according to the at least one credential indexed in the
credential index and the recipient communicating the service level to the sender (using
a certified trusted authority 26 fig.1 to process participant data information, see col.1 line
17 to col.8 line 28 and col.25 line 7 to col.26 line 41).

As to claim 4, Spies discloses that the sender communicates a plurality of credential
indices to the recipient (see col.7 line 17 to col.8 line 28 and col.26 lines 14-65).

As to claim 5, Spies discloses the recipient responding to the credential index by
determining a service level according to each of the plurality of credential indices

communicated to the recipient by the sender and communicating the service level

(trusted level) corresponding to at least one of the credential indices to the sender (col.6

line 36 to col.7 line 45 and col.8 lines 10-56).

As to claim 6, Spies discloses that the recipient communicates a service level to the

sender for each credential index communicated to the recipient by the sender (see fig.6,

col.6 line 36 to col.7 line 45 and col.12 lines 1-59).

As to claims 7-9, Spies discloses that the credential comprising a digital credential,

indices to a plurality of credentials and the sender selecting a credential index from a

plurality of available credential indices (see fig.4, col.6 line 36 to col.7 line 45 and col.12

lines 1-59).

As to claim 10, Spies discloses a method of providing a service over a distributed

electronic network, comprising:

a user (22a fig.1) communicating to a service authorizer (credential binding

server 26 fig.1) a credential index comprising an index referring to at least one user-

provided credential about the credential and the service authorizer (26 fig.1) responding

to the index communicated by the user by selecting at least one of the credentials from

the index of at least one credential provided by the user (22a fig.1) (sending and

exchanging credential information, see fig.1, abstract, col.5 line 21 to col.6 line 24).

the service authorizer responding to the index communicated by the user by

communicating to the user an indication of the selected at least one credential and the

user responding to the indication of selected at least one credential by providing to the

service authorizer at least one credential corresponding to the selected at least one

credential and the service authorizer responding to the at least one credential

corresponding to the selected at least one credential provided to the user by authorizing

provision of the service to the user (providing secure and credential information

between participants, see also fig.2, col.6 line 36 to col.7 line 28 and col.11 line 22 to

col.12 line 63).

Spies does not specifically disclose an index further comprising credential information

differing substantially from the credential such that the credential is not disclosed by the

index. However, Scheidt discloses an index further comprising credential information

differing substantially from the credential (credential that restrict access) such that the

credential is not disclosed by the index (using selecting "Secret" from the security level

category as a credential during encryption would limit readership of the encrypted object

to those who have read access to the "Secret" credential, see fig.3, col.5 line 31 to col.6

line 58 and col.10 lines 10-65). It would have been obvious to one of the ordinary skill

in the art at the time the invention was made to implement Scheidt's secrete credentials

into the computer system of Spies to restrict accesses to data information because it

would have provided sensitivity level or multiple-level access control such that access to

credentials id dependant on the method of member identification and enforced domain

authority dictated policies for multiple-level access control by credential category.

As to claim 11, Spies discloses a computer readable memory configured so that it can be used to direct a computer to:

communicate a recipient (22a fig.1) a credential index comprising an index referring to at least one user provided credential and receive from the recipient an indication of at least one credential selected by the recipient from the index (sending and exchanging credential information between users, see fig.1, abstract, col.5 line 21 to col.6 line 24).

provide to the recipient (22a fig.1) at least one credential corresponding to the selected at least one credential (providing secure and credential information between participants, see also fig.2, col.6 line 36 to col.7 line 28).

Spies does not specifically disclose an index further comprising credential information differing substantially from the credential such that the credential is not disclosed by the index. However, Scheidt discloses an index further comprising credential information differing substantially from the credential (credential that restrict access) such that the credential is not disclosed by the index (using selecting "Secret" from the security level category as a credential during encryption would limit readership of the encrypted object to those who have read access to the "Secret" credential, see fig.3, col.5 line 31 to col.6 line 58 and col.10 lines 10-65). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Scheidt's secrete credentials into the computer system of Spies to restrict accesses to data information because it

would have provided sensitivity level or multiple-level access control such that access to

credentials id dependant on the method of member identification and enforced domain

authority dictated policies for multiple-level access control by credential category.

As to claim 12, Spies discloses a computer readable memory configured so that

can be used to direct a computer to:

receive from a sender (22b fig.1) a credential index comprising an index referring

to at least one credential and select from the index received from the sender at least

one credential (sending and exchanging credential information between users, see fig.1,

abstract, col.5 line 21 to col.6 line 24).

enable an action on receipt said at least one credential from the sender

(providing secure and credential information between participants, see also fig.2, col.6

line 36 to col.7 line 28).

Spies does not specifically disclose an index further comprising credential information

differing substantially from the credential such that the credential is not disclosed by the

index. However, Scheidt discloses an index further comprising credential information

differing substantially from the credential (credential that restrict access) such that the

credential is not disclosed by the index (using selecting "Secret" from the security level

category as a credential during encryption would limit readership of the encrypted object

to those who have read access to the "Secret" credential, see fig.3, col.5 line 31 to col.6

line 58 and col.10 lines 10-65). It would have been obvious to one of the ordinary skill

in the art at the time the invention was made to implement Scheidt's secrete credentials

into the computer system of Spies to restrict accesses to data information because it would have provided sensitivity level or multiple-level access control such that access to credentials id dependant on the method of member identification and enforced domain authority dictated policies for multiple-level access control by credential category.

As to claim 13, Spies discloses a processor for generating a digital credential index, the index comprising a data structure for providing an index to at least one user provided credential (sending and exchanging credential information, see fig.1, abstract, col.5 line 21 to col.6 line 24), whereby at least one credential can be selected on the basis of information provided within the data structure (providing secure and credential information between participants, see also fig.2, col.6 line 36 to col.7 line 28). Spies does not specifically disclose an index further comprising credential information differing substantially from the credential such that the credential is not disclosed by the index. However, Scheidt discloses an index further comprising credential information differing substantially from the credential (credential that restrict access) such that the credential is not disclosed by the index (using selecting "Secret" from the security level category as a credential during encryption would limit readership of the encrypted object to those who have read access to the "Secret" credential, see fig.3, col.5 line 31 to col.6 line 58 and col.10 lines 10-65). It would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Scheidt's secrete credentials into the computer system of Spies to restrict accesses to data information because it would have provided sensitivity level or multiple-level access control such that access to

credentials id dependant on the method of member identification and enforced domain authority dictated policies for multiple-level access control by credential category.

As to claim 14, Spies discloses that the data structure provides indices to a plurality of credentials (see col.25 lines 7-53).

Claims 15 and 16 are rejected for the same reasons set forth in claims 11 and 12 respectively.

Response to Arguments

5.   Applicant's arguments with respect to claims 1-16 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

6.   Claims 1-16 are rejected.

7.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khanh Dinh whose telephone number is (571) 272-3936. The examiner can normally be reached on Monday through Friday from 8:00 A.m. to 5:00 P.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung, can be reached on (571) 272-3939. The fax phone number for this group is (571) 273-8300.

A shortened statutory period for reply is set to expire THREE months from the mailing date of this communication. Failure to response within the period for response will cause the application to become abandoned (35 U. S. C . Sect. 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(A).

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Khanh Dinh
Patent Examiner
Art Unit 2151
7/10/2005